Рубрика 2. Методы и системы защиты информации, информационная безопасность

УДК 004.056.5:004.7

Д. Г. Галустян [1], С. А. Соколов [1]
[1]ФГАОУ ВО «РГУ нефти и газа (НИУ) имени И. М. Губкина», г. Москва, Российская Федерация

ВОПРОСЫ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ RIPv2 НА СЕТЕВЫХ УСТРОЙСТВАХ

Аннотация. Статья посвящена исследованию уязвимостей протокола маршрутизации RIPv2 и способов обеспечения его защищенной эксплуатации на сетевых устройствах. Актуальность работы обусловлена тем, что RIPv2 продолжает применяться в учебных, корпоративных и специализированных сетях, а его дистанционно-векторная логика делает протокол чувствительным к подмене маршрутной метрики. Рассматривается сценарий атаки, при котором злоумышленник, имеющий доступ к общему L2-сегменту, формирует с помощью Scapy поддельные RIPv2-пакеты с заниженным количеством переходов и тем самым воздействует на выбор маршрута. В качестве методологической основы использованы анализ спецификаций RIP/RIPv2, документации производителей сетевого оборудования и лабораторное моделирование на маршрутизаторах Cisco, MikroTik и Eltex. Экспериментальная часть включает проверку работы протокола без аутентификации, с текстовым паролем и с криптографической MD5-аутентификацией по RFC 2082. Дополнительно рассматриваются ограничения применяемых механизмов защиты, особенности конфигурирования устройств разных производителей и влияние ложных обновлений на доступность пользовательских подсетей. Показано, что отсутствие защиты и применение открытого пароля не препятствуют внедрению ложных маршрутов, тогда как MD5-аутентификация отклоняет неподтвержденные обновления и снижает риск нарушения связности. Сформулированы практические рекомендации по безопасной настройке RIPv2, включающие применение ключевых цепочек, фильтрацию маршрутов, ограничение RIP-сегментов и регулярный аудит таблиц маршрутизации. Выработанные меры ориентированы на практическое применение в учебных стендах, сегментах малого предприятия и инфраструктурах, где отказ от RIPv2 пока невозможен.

Ключевые слова: RIPv2, маршрутизация, аутентификация, MD5, Scapy, сетевая безопасность, подмена метрики.

Введение

Несмотря на широкое распространение более современных протоколов маршрутизации (OSPF, EIGRP), протокол RIPv2 сохраняет практическую значимость в ряде специфических случаев. Во-первых, он продолжает использоваться в legacy-инфраструктурах, где переход на более современные протоколы нецелесообразен или невозможен. Во-вторых, RIPv2 часто встречается в промышленных сетях и специализированном оборудовании, где поддержка OSPF может отсутствовать.

RIPv2 расширяет классический RIP за счёт передачи масок подсетей, маршрутов по умолчанию, тегов маршрутов и поля аутентификации, сохраняя при этом дистанционно-векторный алгоритм и ограничение по числу переходов (метрика – от 1 до 15 hop’ов). RIPv2 работает поверх UDP-транспорта (порт 520), отправляя периодические multicast-обновления на устройства, не обеспечивая шифрования содержимого сообщений. Спецификация предусматривает три варианта аутентификации обновлений маршрутов: отсутствие аутентификации, пароль в открытом виде и криптографическая аутентификация на основе MD5. Документация крупных производителей сетевых устройств подчёркивает, что по умолчанию аутентификация RIPv2 отключена. В других случаях используется текстовая строка, при этом рекомендуется переход на MD5 или аналогичные криптографические методы, так как пароль в открытом виде легко перехватывается и впоследствии используется для формирования поддельных пакетов маршрутизации. Развитие средств анализа и генерации сетевого трафика, таких как Scapy, существенно упростило задачу злоумышленнику, таким образом, имея доступ к L2-сегменту, можно не только отправлять произвольные RIPv2-пакеты, но и целенаправленно подменять значения количества hop’ов, таким образом изменяя таблицу маршрутизации атакуемого устройства.

Следовательно, вопросы корректной настройки и защиты RIPv2, особенно в части противодействия атакам с подменой метрики маршрутов, остаются актуальными для значительного числа реальных сетей.

Объект исследования: безопасность сетевых устройств сетевого уровня (L3), использующих протокол маршрутизации RIPv2.

Предмет исследования: механизмы защиты RIPv2 на сетевом оборудовании от атак на основе подмены количества hop’ов в RIPv2-пакетах с помощью инструментов пакетной генерации, методы их реализации и эффективность в реальной инфраструктуре.

Цель исследования: Анализ уязвимостей RIPv2, связанных с подменой метрики, и существующих механизмов его защиты; разработка и экспериментальная проверка комплекса конфигурационных мер, повышающих устойчивость сетевой инфраструктуры к таким атакам.

Обзор и методология исследования

RIPv2 является развитием классического RIP с поддержкой CIDR, меток маршрута, multicast-доставки обновлений и поля для аутентификации. Протокол реализует дистанционно-векторный алгоритм, периодически рассылая таблицу маршрутов, где для каждого префикса указываются сеть, маска и метрика – численное значение, интерпретируемое как количество переходов (hop count) до назначения. Разновидности атак на RIPv2 представлены в таблице 1. Оценка угроз производилась в соответствии с открытым стандартом для расчёта количественных оценок уязвимостей – CVSS (Common Vulnerability Scoring System). Метрики для оценки: вектор атаки, сложность атаки, требуемые привилегии.

Таблица 1 – Разновидности атак на RIPv2

№	Название атаки	Описание	Оценка угрозы по CVSS
1	Hop-count route attack (занижение метрики)	Захват трафика, отправка маршрутов с меньшей метрикой	8.2
2	Route Injection (вставка ложных маршрутов)	Перегрузка таблицы маршрутизации, добавление несуществующих сетей в RIP-обновления	7.5
3	Route Poisoning spoof	Отправка обновлений с метрикой 16 от имени соседа, удаление маршрута из таблицы	6.5
4	Neighbor Spoofing	Отправка RIP-пакета с поддельным IP соседа, полный контроль над маршрутизацией	9.1

В данной работе рассматривается сценарий атакующего воздействия атаки hop-count spoofing, так как она является наиболее популярной и простой, но в то же время оказывает критическое воздействие на сетевые устройства. Суть атаки заключается в формировании поддельных RIPv2-сообщений, где для интересующих подсетей указываются намеренно заниженные метрики (1–2 хопа). Поскольку классический RIP всегда выбирает маршрут с минимальной метрикой, такие записи воспринимаются как более предпочтительные, что позволяет злоумышленнику:

– перехватывать трафик к целевым подсетям;

– перенаправлять трафик в пустоту, не маршрутизируя его далее;

– провоцировать нестабильность маршрутизации за счёт частой смены значения метрик.

Для генерации подобных пакетов можно использовать Scapy (библиотеку на Python для конструирования, модификации и отправки произвольных сетевых пакетов). Инструмент Scapy предоставляет реализацию протокола RIP/RIPv2 как отдельного слоя, что позволяет программно задавать любые значения метрики и других полей.

Основные гипотезы исследования:

– в сетях, где RIPv2 работает без аутентификации или использует текстовый пароль, злоумышленник, имеющий доступ к L2-сегменту и инструментам рассылки пользовательских пакетов, может успешно подменять количество hop’ов в RIPv2-пакетах, внедряя ложные маршруты и нарушая доступность устройств;

1. Включение MD5-аутентификации на всех соседствах RIPv2 существенно усложняет или делает невозможной подмену количества hop’ов с неподтверждённых устройств, однако не исключает риск атак при компрометации ключа.

– комплекс описанных мер защиты существенно снижает вероятность успешной атаки и уменьшает её последствия для маршрутизации.

Рубрика 2. Методы и системы защиты информации, информационная безопасность

Методы исследования

Тип исследования: анализ безопасности протокола с элементами экспериментального тестирования в лабораторной среде.

Характеристика среды исследования: лабораторная сетевая инфраструктура, включающая физические коммутаторы и маршрутизаторы производителей Cisco, MikroTik, Eltex, а также два PC. На PC установлена операционная система Linux.

Методы сбора данных

– захват и анализ RIPv2-трафика с помощью Wireshark;

– логирование маршрутизаторов (команды просмотра таблиц маршрутизации, режимы debug для RIPv2, журналы аутентификации и безопасности);

– измерение доступности и числа изменений маршрутов при различных сценариях атаки.

Процедура проведения исследования

1. Настройка базовой топологии с использованием RIPv2 без аутентификации.

2. Формирование атакующих RIPv2-пакетов в Scapy с заниженным количеством hop’ов для маршрута и их рассылка.

3. Анализ влияния подмены количества hop’ов на таблицы маршрутизации и доступность сетевых ресурсов.

4. Включение простой текстовой аутентификации, повторение атак с предварительным перехватом пароля и подменой количества hop’ов в аутентифицированных RIPv2-пакетах.

5. Включение MD5-аутентификации на всех линках RIPv2, повторение атак с поддельными пакетами.

6. Сравнительный анализ поведения оборудования разных производителей и эффективности различных комбинаций защитных механизмов.

Методы обработки данных:

Количественный анализ успешности атаки (по критериям изменения маршрутов и потери связности); оценка времени сходимости при штатной работе и в условиях атак; качественный анализ журналов и диагностических сообщений устройств при корректной и некорректной аутентификации RIPv2-пакетов.

Основные этапы экспериментального исследования

Лабораторная среда эксперимента

Целью эксперимента является воспроизведение небольшой сети, где RIPv2 используется для обмена маршрутной информацией между несколькими маршрутизаторами, а атакующий узел с Scapy имеет доступ к одному из общих сегментов.

Топология сети

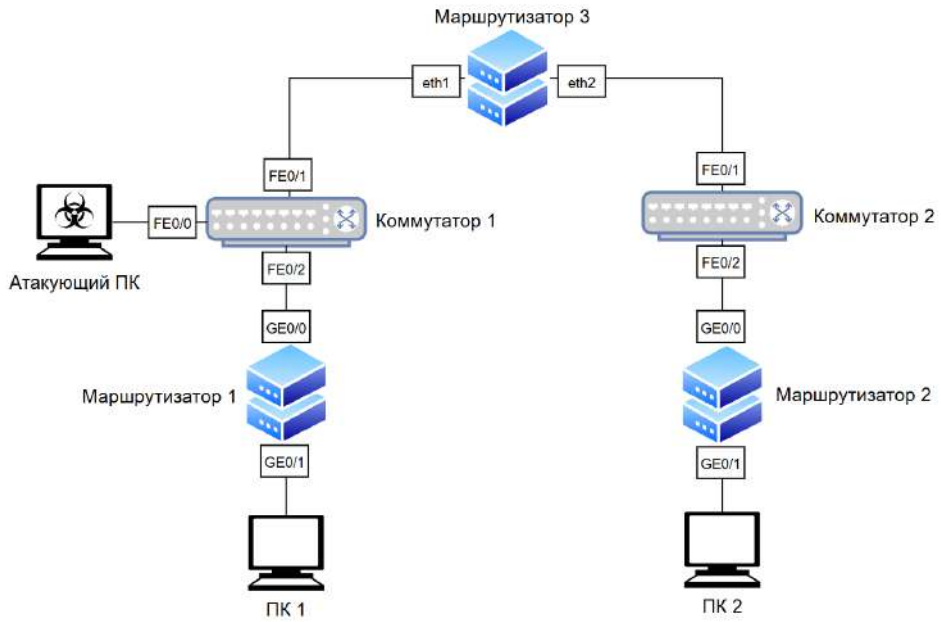

Рис. 1. Топология сети для проведения эксперимента

Конфигурация машин

Для проведения работ необходимо подготовить следующее оборудование:

Сетевое оборудование: коммутатор и маршрутизаторы (Cisco, MikroTik, Eltex).

Рабочие станции:

Атакующий ПК – компьютер на базе ОС Linux.

ПК1 и ПК2 – компьютер с любой операционной системой и сетевым интерфейсом.

Соединительные компоненты: Ethernet-кабели для подключения рабочих станций к коммутаторам.

Проведём настройку оборудования:

Подключаем атакующий ПК к коммутатору как показано в топологии. Атакующий ПК должен находиться в одной подсети с маршрутизатором, чтобы он воспринимал получаемые пакеты как исходящие от соседних устройств. Команды, используемые для настройки маршрутизатора каждого производителя представлены в таблице 2.

Таблица 2 – Команды первичной настройки маршрутизаторов

Блок команд	**Cisco (Маршрутизатор 1)**	**Eltex (Маршрутизатор 2)**	**MikroTik (Маршрутизатор 3)**
Настройка первого интерфейса	enable configure terminal interface GigabitEthernet0/0 ip address 192.168.100.1 255.255.255.252 no shutdown exit	enable configure terminal interface gigabitethernet 0/0 ip address 192.168.200.1 255.255.255.252 no shutdown exit	interface ethernet set ether1 disabled=no ip address add address=192.168.100.2/30 interface=ether1
Настройка второго интерфейса	interface GigabitEthernet0/1 ip address 10.10.10.1 255.255.255.0 no shutdown exit	interface gigabitethernet 0/1 ip address 20.20.20.1 255.255.255.0 no shutdown exit	interface ethernet set ether2 disabled=no ip address add address=192.168.200.2/30 interface=ether2
Настройка RIPv2	router rip version 2 no auto-summary network 192.168.100.0 network 10.0.0.0 exit write memory	router rip version 2 no auto-summary network 192.168.200.0 network 20.20.20.0 exit write	routing rip set enabled=yes routing rip interface add interface=ether1 routing rip network add network=192.168.100.0/30 routing rip network add network=192.168.200.0/30

Моделирование атаки

Атакующий ПК посылает серию RIPv2-пакетов, в которых метрика имеющихся в таблице адресов предоставляется как более оптимальная. Это приводит к пересчёту таблиц маршрутизации для выбора более предпочтительного маршрута. Далее приведен листинг скрипта авторского написания на Scapy, генерирующий ложный RIPv2 пакет в лабораторной среде. В реальном скрипте параметры должны передаваться как аргументы, чтобы обеспечить универсальность работы инструмента.

```
from scapy.all import *
# IP адрес атакуемого устройства
target_ip = "192.168.100.2"
# Параметры ложного пакета: метрика и сеть
fake_metric = 1
network_addr = "10.10.10.10"
network_mask = "255.255.255.0"
# Формирование записи RIP для пакета
rip_entry = RIPEntry(
  AF=2,
  addr=network_addr,
  mask=network_mask,
  metric=fake_metric
```

```
)
# Создание пакета RIPv2
rip_packet = IP(dst=target_ip) / \
        UDP(sport=520, dport=520) / \
        RIP(cmd=2, version=2) / \
        rip_entry
```

Поддельные RIP-пакеты успешно формируются и отправляются с использованием инструмента Scapy. Маршрутизаторы начали получать некорректные записи с пониженными значениями метрик, что привело к появлению ложных маршрутов в их таблицах. Наблюдение за работой устройств в режиме отладки, показывает, что пакеты принимаются и обрабатываются маршрутизатором.

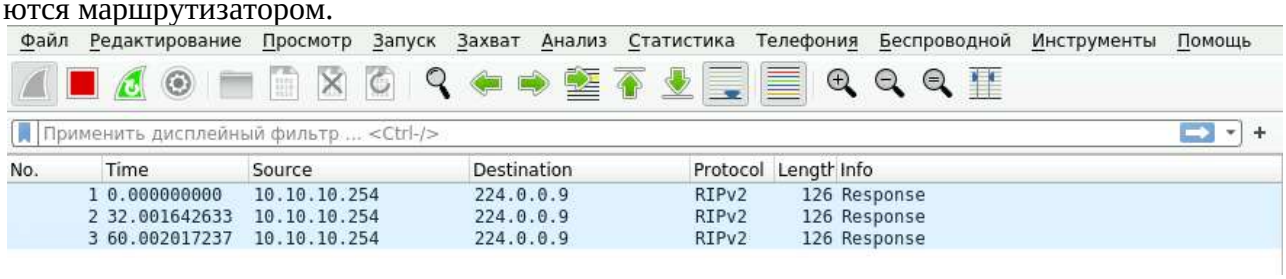

Рис. 2. Захват трафика на атакующем ПК до атаки.

Анализ трафика в Wireshark на атакующем ПК подтверждает изменение таблицы маршрутизации: ПК становится новым next-hop для объявленной сети. Маршрутизатор начинает перенаправлять через него соответствующий трафик, вследствие чего ICMP пакеты появляются в Wireshark.

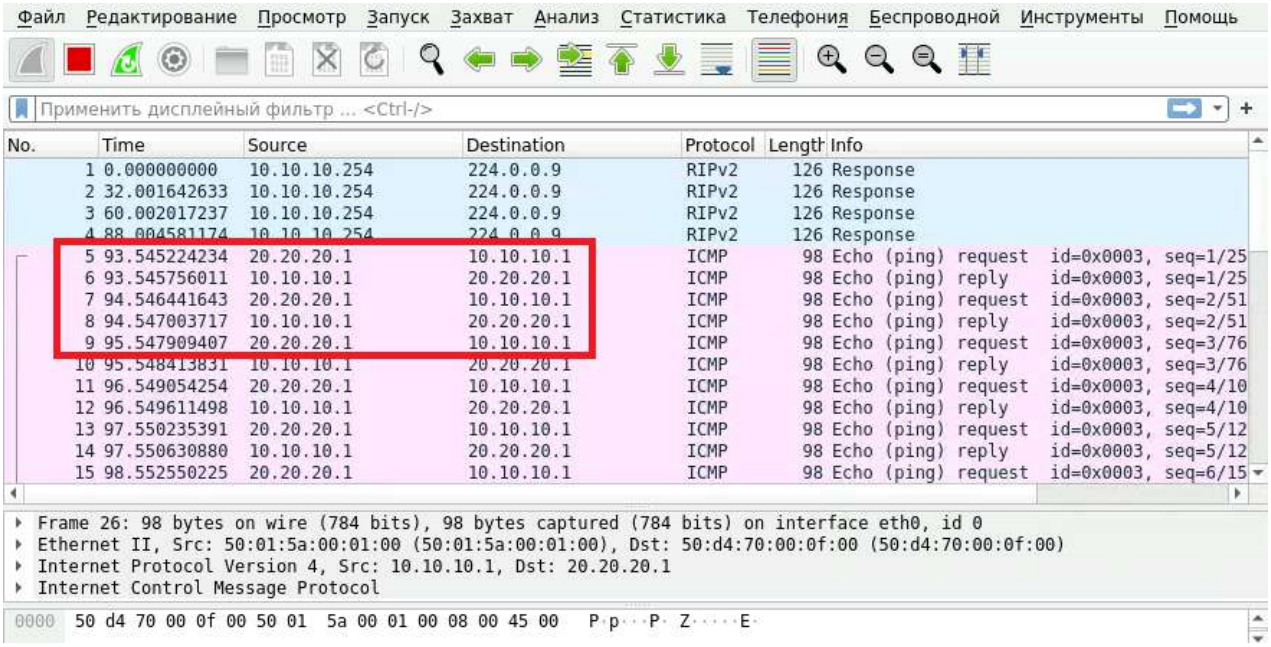

Рис. 3. Захват трафика на атакующем ПК после атаки.

Реализация защитных механизмов

Механизм 1. Аутентификация с использованием текстового пароля (Plain Text Authentication).

Одним из базовых механизмов защиты RIPv2 является применение текстовой аутентификации. В этом режиме в каждый RIP-пакет включается специальная запись, содержащая пароль в открытом виде (plain text). Маршрутизатор принимает маршрутную информацию только в том случае, если значение пароля совпадает с локально настроенным.

Команды для настройки аутентификации с использованием текстового пароля представлены в таблице 3.

Таблица 3 – Команды для настройки аутентификации с использованием текстового пароля

Блок команд	**Cisco (Маршрутизатор 1)**	**Eltex (Маршрутизатор 2)**	**MikroTik (Маршрутизатор 3)**
Создание key chain	enable configure terminal key chain RIP-PLAIN key 1 key-string testpass exit	enable configure terminal key chain RIP-PLAIN key 1 key-string testpass exit	1) routing rip interface add interface=ether1 authentication=plain password=testpass
Включение аутентификации	1) interface GigabitEthernet0/0 2) ip rip authentication mode text 3) ip rip authentication key-chain RIP-PLAIN 4) exit 5) write memory	1) interface gigabitethernet 0/1 2) ip rip authentication mode text 3) ip rip authentication key-chain RIP-PLAIN 4) exit 5) write	1) routing rip interface set [find interface=ether1] authentication=plain password=testpass

На рис. 4 изображен анализ захваченного трафика, который подтверждает корректную работу включенной защиты на основе простого текстового ключа.

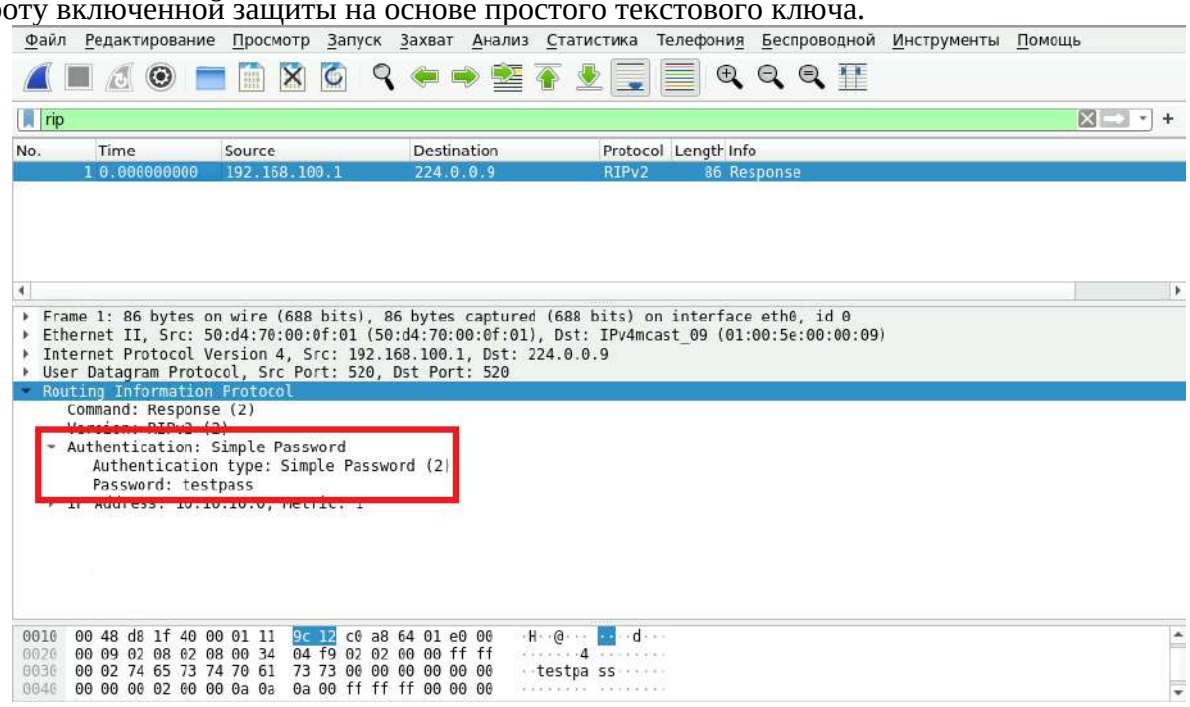

Рис. 4. RIPv2 пакет, защищенный с помощью Plain Text Authentication.

Механизм 2. Аутентификация на основе MD5.

Для повышения устойчивости к подделке RIP-сообщений существует более надёжный метод – аутентификация на основе хеш-функции MD5. Этот механизм определён в RFC 2082 и значительно повышает безопасность RIPv2. Маршрутизатор проверяет хеш каждого полученного RIP-пакета. Если значение не совпадает – пакет считается поддельным и отклоняется.

Команды для настройки аутентификации на основе MD5 представлены в таблице 4.

Таблица 4 – Команды для настройки аутентификации на основе MD5

Блок команд	Cisco (Маршрутизатор 1)	Eltex (Маршрутизатор 2)	MikroTik (Маршрутизатор 3)
Создание key chain	enable configure terminal key chain RIP-MD5 key 1 key-string MD5secretkey exit	enable configure terminal key chain RIP-MD5 key 1 key-string MD5secretkey exit	routing rip interface add interface=ether1 authentication=md5 password=MD5secretkey
Включение аутентификации	interface GigabitEthernet0/0 ip rip authentication mode md5 ip rip authentication key-chain RIP-MD5 exit	interface gigabitethernet 0/1 ip rip authentication mode md5 ip rip authentication key-chain RIP-MD5 exit	routing rip interface set [find interface=ether1] authentication=md5 password=MD5secretkey

На рис. 5 изображен анализ захваченного трафика, который подтверждает корректную работу включенной защиты на основе MD5.

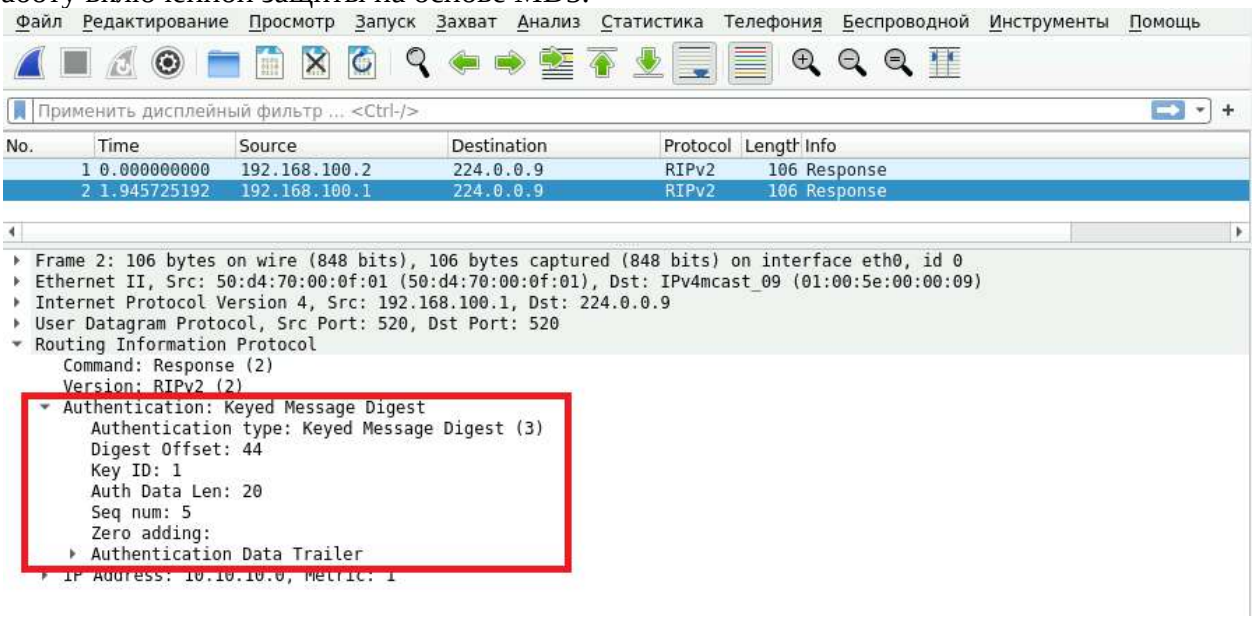

Рис. 5. RIPv2 пакет, защищенный с помощью MD5 Authentication.

Результаты исследования

Экспериментальная часть работы показала, что RIPv2 крайне чувствителен к подмене количества hop’ов в пакетах, формируемых с помощью сторонних утилит, если протокол не защищён механизмами аутентификации и фильтрации. В исходной конфигурации, когда аутентификация RIPv2 отсутствовала, любой узел в общем L2-сегменте мог сгенерировать RIPv2-пакеты с произвольными маршрутами и заниженными значениями метрики. При рассылке таких пакетов по мультикаст-адресу 224.0.0.9 маршрутизатор принимал их как обычные обновления, заносил в таблицу маршрутизации новые записи и выбирал именно этот маршрут как оптимальный, поскольку количество hop’ов, установленное злоумышленником, было меньше, чем у реальных путей. В результате трафик между пользовательскими подсетями начинал проходить через атакующий узел. Связь между ПК была нарушена.

При включении текстовой аутентификации ситуация принципиально не изменилась. Анализ трафика RIPv2 показал, что строка пароля передаётся в открытом виде и без труда считывается (см. рис. 4). После этого атакующий, зная корректное значение поля аутентификации, мог воспроизвести те же самые сценарии подмены количества hop’ов, добавив соответствующую текстовую строку в формируемые пакеты. Маршрутизаторы воспринимали такие сообщения как полностью корректные и продолжали принимать ложные маршруты с

подменённой метрикой. Таким образом, текстовая аутентификация практически не повысила устойчивость сети к рассматриваемому типу атаки.

Ситуация принципиально изменилась при переходе на криптографическую аутентификацию (MD5 по RFC 2082). После настройки ключевых цепочек на всех маршрутизаторах и привязки их к интерфейсам RIPv2 пакеты, сформированные на атакующем ПК без знания секретного ключа, перестали оказывать какое-либо влияние на маршрутизацию.

Хотя MD5-аутентификация в RIPv2 значительно повышает стойкость протокола по сравнению с незащищённым текстовым паролем, описанным выше, алгоритм MD5 считается устаревшим с точки зрения криптографии. Его слабость заключается в уязвимостях его хеш-функции, в первую очередь – наличием эффективных и распространенных методов построения коллизий, когда злоумышленник может создать другой набор данных с тем же хеш-значением. Несмотря на существование более современного и криптостойкого стандарта RFC 4822, описывающего механизм аутентификации на основе HMAC-SHA, ни один из тестируемых маршрутизаторов его не поддерживает на программном уровне. Исходя из этого, практическая рекомендация к использованию MD5 для аутентификации обусловлена не его достаточной степенью защиты, а конкретными ограничениями сетевого оборудования.

Сравнение поведения устройств разных производителей (Cisco, MikroTik, Eltex) показало, что при одинаковой логике защиты их устойчивость к подмене количества hop’ов оказывается сопоставимой. Следует отметить, что заметное отличие в логике настройки было характерно только для MikroTik, в то время как интерфейсы конфигурирования Cisco и Eltex практически идентичны.

Заключение

Проведённый анализ протокола RIPv2, стандартов аутентификации и лабораторное моделирование атак с подменой количества hop’ов при помощи Scapy позволили сформулировать следующие выводы по заявленным гипотезам.

Гипотеза 1 подтверждена. RIPv2 без аутентификации или с использованием простой текстовой аутентификации подвержен атакам, основанным на подмене значения количества hop’ов в RIPv2-пакетах: злоумышленник может объявлять свой маршрут к целевым подсетям и нарушать доступность сервисов.

Гипотеза 2 подтверждена. MD5-аутентификация по RFC 2082 эффективно предотвращает подмену количества hop’ов с неавторизованных устройств, но её надёжность зависит от секретности ключей.

Гипотеза 3 подтверждена. Комбинация криптографической аутентификации с топологическими ограничениями и фильтрацией маршрутов существенно повышает устойчивость сети к атакам на основе подмены количества hop’ов и позволяет минимизировать последствия таких атак.

Чек-лист для безопасного использования RIPv2:

– анонсировать только необходимые интерфейсы, остальные перевести в режим passive-interface;
– применять MD5-аутентификацию;
– использовать key-chain для управления ключами;
– регулярно менять криптографические ключи;
– исключить возможность попадания злоумышленника в RIP-сегмент;
– использовать анализаторы трафика RIP, регулярно проверять таблицы маршрутизации, логировать изменения.

Практическая значимость и рекомендации:

Полученные результаты обладают прикладным характером и могут быть использованы и внедрены в корпоративных и учебных сетях, где задействован RIPv2. На основе анализа сформулированы следующие рекомендации:

– обязательное использование криптографической аутентификации RIPv2. В реальных сетях необходимо применять MD5 или более современные алгоритмы (при наличии поддержки в оборудовании);

– фильтрация маршрутов и контроль метрик. Запрет приёма маршрута по умолчанию от неподходящих соседей, а также аномальных префиксов и метрик;

– регулярный аудит конфигураций и журналов. Проверка наличия аутентификации, отсутствие подозрительных изменений таблиц маршрутизации и нестандартных значений количества hop’ов.

Направления дальнейших исследований

Анализ устойчивости RIPv2 аутентификации к современным методам криптоанализа и атакам подбора ключей, в том числе при использовании инструментов пакетной генерации.

Исследование комбинированных атак, совмещающих подмену количества hop’ов в RIPv2 с отравлением ARP, DHCP и другими атаками на протоколы канального и сетевого уровней.

Библиографический список

1. Уймин, А. Г. Применение отечественного сетевого оборудования Eltex и EcoRouter в рамках специальности 09.02.06 «Сетевое и системное администрирование». Вопросы импортозамещения и подготовки квалифицированных кадров в сетевом оборудовании / А. Г. Уймин, И. М. Толмачев // Автоматизация и информатизация ТЭК. – 2025. – № 11(628). – С. 58–62. – EDN DMHQJU.
2. Convery, D. Network Security Architectures [Электронный ресурс] / D. Convery, J. Choe // Cisco Press. – 2004. – URL: https://www.ciscopress.com/articles/article.asp?p=102157 (дата обращения: 25.11.2025).
3. Perlman, R. Interconnections: Bridges, Routers, Switches, and Internetworking Protocols / R. Perlman. – 2nd ed. – Reading, Mass. : Addison-Wesley, 2000. – 538 p.
4. Vyncke, E. LAN Switch Security: What Hackers Know About Your Switches / E. Vyncke. – Indianapolis, IN : Cisco Press, 2008. – 336 p.
5. Baker, F. RFC 2082: RIP-2 MD5 Authentication / F. Baker, R. Atkinson. – Internet Engineering Task Force, 1997. – URL: https://datatracker.ietf.org/doc/html/rfc2082 (дата обращения: 25.11.2025).
6. Malkin, G. RFC 2453: RIP Version 2 / G. Malkin. – Internet Engineering Task Force, 1998. – URL: https://datatracker.ietf.org/doc/html/rfc2453 (дата обращения: 25.11.2025).
7. Красноперов, К. Ю. Отличия между протоколами RIPv1 и RIPv2 / К. Ю. Красноперов // Академическая публицистика. – 2023. – № 10-2. – С. 88–90. – EDN BXFIGT.

References

1. Uymin, A. G., & Tolmachev, I. M. (2025). Application of domestic network equipment Eltex and EcoRouter within the specialty 09.02.06 "Network and System Administration": Issues of import substitution and training of qualified personnel in network equipment. Automation and Informatization of the Fuel and Energy Complex, (11), 58–62.
2. Convery, D., & Choe, J. (2004). Network security architectures. Cisco Press. Retrieved November 25, 2025, from https://www.ciscopress.com/articles/article.asp?p=102157
3. Perlman, R. (2000). Interconnections: Bridges, routers, switches, and internetworking protocols (2nd ed.). Addison-Wesley.
4. Vyncke, E. (2008). LAN switch security: What hackers know about your switches. Cisco Press.
5. Baker, F., & Atkinson, R. (1997). RIP-2 MD5 authentication (RFC 2082). Internet Engineering Task Force. https://datatracker.ietf.org/doc/html/rfc2082
6. Malkin, G. (1998). RIP version 2 (RFC 2453). Internet Engineering Task Force. https://datatracker.ietf.org/doc/html/rfc2453
7. Krasnoperov, K. Yu. (2023). Differences between RIPv1 and RIPv2 protocols. Akademicheskaya Publitsistika, (10-2), 88–90.

Информация об авторах

Галустян Д. Г. — студент 3 курса факультета «Комплексная безопасность топливно-энергетического комплекса», ФГАОУ ВО «РГУ нефти и газа (НИУ) имени И. М. Губкина», г. Москва, e-mail: galustyan.dg@gmail.com.

Соколов С. А. — студент 3 курса факультета «Комплексная безопасность топливно-энергетического комплекса», ФГАОУ ВО «РГУ нефти и газа (НИУ) имени И. М. Губкина», г. Москва, e-mail: sokolov.sa@gmail.com.

ISSUES OF ENSURING RIPv2 PROTECTION ON NETWORK DEVICES

Galustyan D. G.[1], Sokolov S. A.[1]

[1]National University of Oil and Gas «Gubkin University», Moscow, Russian Federation

Abstract. The article examines the security issues of RIPv2 routing protocol operation on network devices and focuses on attacks based on route metric spoofing. The relevance of the study is determined by the fact that RIPv2 is still used in educational, corporate and specialized network segments, while its distance-vector logic makes route selection dependent on the advertised hop count. The paper considers an attacker who has access to a common Layer 2 segment and uses Scapy to generate forged RIPv2 packets with artificially reduced metrics. The methodological basis of the research includes analysis of RIP/RIPv2 specifications, vendor documentation and laboratory modelling on Cisco, MikroTik and Eltex equipment. The experimental part compares three operating modes: RIPv2 without authentication, RIPv2 with a plain-text password and RIPv2 with MD5 cryptographic authentication according to RFC 2082. The results show that the absence of authentication and the use of a readable password do not prevent false route injection, because an attacker can reproduce valid-looking updates and influence routing tables. MD5 authentication rejects unauthorised updates and significantly reduces the risk of traffic interception or loss of connectivity, although its effectiveness depends on key secrecy and equipment support. Practical recommendations are proposed for safer RIPv2 deployment, including key-chain management, route filtering, isolation of RIP segments and regular auditing of routing tables and logs.

Keywords: RIPv2, routing, authentication, MD5, Scapy, network security, metric spoofing.

Information about the authors

Galustyan D. G. — 3rd-year student, Faculty of Integrated Security of the Fuel and Energy Complex, Gubkin Russian State University of Oil and Gas (National Research University), Moscow, e-mail: galustyan.dg@gmail.com.

Sokolov S. A. — 3rd-year student, Faculty of Integrated Security of the Fuel and Energy Complex, Gubkin Russian State University of Oil and Gas (National Research University), Moscow, e-mail: sokolov.sa@gmail.com.